REMARKS

Claims 14, 23, 34, 42 and 43 are amended. No new claims are added. Claims 1-49 are pending for consideration. In view of the following remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

The Objection to the Drawings

The specification has been amended to include the reference designators 306a, 806, and 814. Applicant thanks the Examiner for his attention to detail and respectfully requests that the drawing objection be withdrawn.

The Objection to the Specification

Applicant has capitalized each letter of and added the encircled R to each trademark used to identify the origin of goods and/or services specified in the application. Applicant respectfully submits that the mere usage of corporate names, for example, referring to a particular company's employees, does not warrant the use of the encircled R because the Applicant does not use the corporate name to identify the origin of any particular goods or services. Accordingly, Applicant respectfully requests that the specification objection be withdrawn.

The § 102 Rejections

Claims 1-6, 8-17, 19-29 and 33-49 stand rejected under 35 U.S.C. § 102(b) as being anticipated by WIPO Patent Application No. 99/01969 to Xu et al. (hereinafter "Xu").

The § 103 Rejections

Claims 7 and 18 stand rejected under § 103(a) as being unpatentable by Xu in view of U.S. Patent No. 5,742,763 to Jones (hereinafter "Jones").

Claim 30 stands rejected under § 103(a) as being unpatentable by Xu in view of WIPO Application No. 98/32254 to Scholnick et al. (hereinafter "Scholnick").

Claims 31 and 32 stand rejected under § 103(a) as being unpatentable by Xu in view of U.S. Patent No. 5,742,598 to Dunn et al. (hereinafter "Dunn").

Applicant's Disclosure

Before Applicant specifically addresses the Office's rejections, the following discussion is provided to assist the Office in appreciating the patentable distinctions between Applicant's claimed embodiments and the cited references.

As a starting point, consider the traditional network paradigm for Internet access. Traditionally, there are a couple of different ways for an individual to access the Internet. First, the individual might have a personal account with an Internet Service Provider (ISP) whereby they can access the Internet through, for example, their home computer. Their home

computer establishes a link with the ISP through a modem or special communication line. Once the link is established, generally over a wired line, they can typically use ISP-provided software to browse the Internet. In this example, an individual's Internet access is either tied to their wired link provider, or to the ISP through which they have their account. Second, an individual might be able to access the Internet through a network that is provided and maintained by their employer. While they are at work, they can access the Internet through the use of employer-provided resources. In this example, an individual's Internet access is tied to their employer and/or their employer's resources.

Neither of these paradigms provides an individual with the freedom to access the Internet from any location and ***without any dependence on a particular ISP*** or their company. Rather, Internet accessibility for these individuals is necessarily tied to either or both of (1) signing up for an account with a particular ISP for Internet access, or (2) being a member of a particular corporation through which Internet access is provided. It would be desirable to eliminate the dependence of Internet access on either or both of these elements. For example, when Internet access is provided in public places, it is typically tied to a particular ISP and the consumer really has no choices whatsoever concerning such things as quality of service, type of service available, and the like.

Conversely, Applicant's architecture enables a user to freely move about from host organization to host organization, ***without having their Internet access inextricably tied to any one particular ISP*** or to a particular company such as their employer. This system permits a much

more individual-centric system that promotes user mobility, as will become apparent below. Another advantage of this architecture is that once a user is authenticated, they can move freely about without having to re-authenticate themselves to the system. Another advantageous feature of the above architecture is that users can have freedom of choice. That is, the authentication/negotiation component can be programmed to negotiate for services on behalf of the user. For example, a host organization network might have a number of different ISPs (e.g. AT&T, MCI, SPRINT and the like) that are under contract to provide Internet access. A user can specify a particular level of service (i.e. transmission rate and desired cost structure). The authentication/negotiation component then negotiates the desired service level with the particular ISPs. Thus, a user can receive the best deal for their desired parameters. As an example, a particular user may be in a rush (i.e. between flights in an airport) and may need to have the fastest Internet access that is possible. Further, they may be willing to pay a top premium for such access. Once the authentication/negotiation component 110 is notified of these parameters, it can then find ***the ISP that most closely meets the user's parameters***.

The Xu Reference

Xu discloses a system and method for connecting a source of digital data to a computer network. Perhaps a good place to start for an appreciation of Xu's systems and methods is with Xu's Fig. 1 and the related discussion starting on page 6 at line 20. There, Xu instructs that the illustrated communications chassis 20 functions as a gateway between the

CDMA/TDMA wireless network 16 and an Internet service provider (ISP) backbone network 26, the Internet 22, or other computer network such as a corporate or private LAN/WAN 24 via an Ethernet or other local area network ETH and the Internet service provider backbone network 26. The chassis 20 provides the functions needed for terminal equipment connected to a CDMA or TDMA mobile phone to intercommunicate with terminal equipment connected to the PSTN and Internet networks. Xu instructs that the communications chassis 20 is installed at the telephone company central office (TELCO CO) and managed by an Internet Service Provider (ISP). The chassis 20 receives calls from wireless users 12, 14 via the MSC in the wireless network 16 as local calls on the line FR.

Xu describes an advantage of its system on page 7, starting at line 22. There, Xu instructs that the illustrated architecture also allows the Internet Service Provider operating the local communications chassis 20 at the central office to provide Internet access for the ISP's customers and customers of other Internet service providers. This is achieved by use of one or more authentication servers 32A, 32B connected to the Internet service provider's backbone network 26. The authentication servers 32A, 32B perform authentication and access authorization for the first ISP's customers. A second tunneling server 34 is connected via a dedicated line 36 (or LAN or WAN) or otherwise to a second ISP's backbone network 38. In this embodiment, the authentication server 32A has a profile of its customer base for the first ISP managing the communications chassis 20 and can determine whether the remote user dialing into the communications device 20 is allowed to access the Internet 22 via the ISP's backbone 26. If

access is allowed (due to the call originating from one of the first Internet service provider customers), the call is routed through the network 22 to the Internet. If not, then the authentication server 32A directs the authentication request to a second authentication server 40, which determines if the user is a customer of the second Internet service provider. If the user is determined to be a customer of the second Internet service provider, access is granted.

Thus, in Xu's system, the user is required to be affiliated with one of the given ISPs before the user can gain access to its system.

Claims 1-13

Claim 1 recites an authentication system comprising [emphasis added]:

- a host network configured to provide access to the Internet from a public location;
- at least one authentication component communicatively linked with the host network and configured to enable authentication of individual users so that they can access the Internet through the host network, authentication being configured to take place in a manner that is ***independent of any user affiliation with any Internet Service Providers (ISPs)***;
- at least one access module communicatively linked with the one authentication component and configured to enable a user to access the host network; and
- an authentication database communicatively linked to the host network and containing user information that can be used to authenticate a user.

In making out the rejection of claim 1, the Office argues that Xu anticipates this claim. Applicant respectfully but strongly disagrees. Xu does not disclose or suggest authentication being configured to take place

in a manner that is ***independent of any user affiliation with any Internet Service Providers (ISPs)***.

In support of its argument, the Office cites to page 7, lines 22-24, for the proposition that Xu discloses an authentication component which allows connection to "any ISP." This excerpt was reproduced as part of a larger excerpt above but is repeated below for the Office's convenience [emphasis added]:

> The architecture also allows the ***Internet Service Provider operating the local communications chassis*** 20 at the central office to provide Internet access for not only the ISP's customers, but also customers of ***other Internet service providers***.

First, Applicant respectfully submits that this excerpt does not state (or even imply) that Xu's system allows connection to "any ISP." Moreover, even if Xu's system did allow connection to any ISP, that would be quite different from Applicant's claimed subject matter. Applicant's authentication is configured to take place in a manner that is ***independent*** of ***any*** user affiliation with ***any*** Internet Service Providers (ISPs). As noted above in the section entitled "Xu's Disclosure", Xu teaches ***directly away*** from Applicant's claimed subject matter by making authentication ***dependent*** upon user ***affiliation with one of the given ISPs*** before the user can be authenticated.

Accordingly, for at least this reason, this claim is allowable.

Claims 2-13 depend from claim 1 and, as such, are allowable as depending from an allowable base claim. These claims are also allowable

for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested by Xu either alone or in combination with any of the references of record.

For example, **claim 5** recites that the one authentication component is ***not privy*** to any authentication information that passes between the user and the authentication database.

The Office argues that Xu anticipates this claim. Applicant respectfully but strongly disagrees. On page 13, lines 23-31, Xu discloses the following [emphasis added]:

> (1) receiving the digital data at a network access server or communications chassis 20 and ***extracting***, from the digital data, ***network access authentication data*** comprising at least one of the following: (a) a telephone number called by the source 12 of digital data, or (b) a telephone number associated with source of digital data;
>
> (2) ***transmitting the authentication data*** over a local area or wide area computer network connected to the communications device 20 to a network authentication server 32A or 32B for the computer network 24 or 22, the network authentication server linked via the local area or wide area computer network 26 to the communications chassis 20;

Therefore, Xu discloses a communications chassis, which ***is*** privy to authentication information which passes between the user and the authentication database. As such, Xu again teaches ***directly away*** from Applicant's claimed subject matter. For at least this reason, this claim is allowable.

In addition, with respect to **claim 7**, the addition of the Jones reference is not seen to add anything of significance, given the allowability of claim 1.

Claims 14-22

As amended, **claim 14** recites an authentication system for providing authentication for users who desire to access the Internet, the system comprising [emphasis added]:

- at least one host organization network configured to access the Internet, the host organization network comprising one or more subnets each of which comprising:
  - at least one server configured to receive data packets from individual client computing devices and transmit the data packets to the Internet; and
  - a plurality of public access points each of which configured to receive wireless communication from a user that is using a client computing device to wirelessly transmit data packets that are intended for the Internet and provide the wirelessly transmitted data packets to the one server before the data packets are transmitted to the Internet; and
- at least one globally accessible authentication database that contains information that can be used by the database to authenticate a user ***without requiring the user to be affiliated with a particular Internet Service Provider (ISP)***.

Applicant has amended this claim to clarify that authentication of a user ***does not require*** the user to be affiliated with a particular ISP. In making out the rejection of this claim, the Office argues that this claim is anticipated by Xu. However, as noted above, Xu ***does require*** the user to be affiliated with one of the given ISPs before the user can be

authenticated. As such, Xu teaches ***directly away*** from Applicant's claimed subject matter. Accordingly, for at least this reason, this claim is allowable.

Claims 15-22 depend from claim 14 and, as such, are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 14, are neither shown nor suggested by Xu either singly or in combination with any of the references of record.

For example, **claim 16** recites that the one server is ***not privy*** to authentication information that is passed between the client computing device and the globally accessible authentication database. As noted above, Xu teaches ***directly away*** from Applicant's claimed subject matter by teaching that its communication chassis ***is*** privy to authentication information that is passed between the client computing device and the globally accessible authentication database. Accordingly, for at least this reason, this claim is allowable.

As another example, **claim 22** recites that the user is ***unaffiliated*** with any Internet Service Providers (ISPs). As noted above, Xu teaches ***directly away*** from this inventive concept. Xu's Fig. 1 and specification at page 7, lines 22-24, reproduced earlier, specifically teach that only users who ***are affiliated*** with one of the specified ISPs can gain access to the Internet through Xu's system. Accordingly, for at least this reason, this claim is allowable.

In addition, with respect to **claim 18**, the addition of the Jones reference is not seen to add anything of significance, given the allowability of claim 14.

Claims 23-33

As amended, **claim 23** recites an authentication system for providing authentication for users who desire to access the Internet, the system comprising [emphasis added]:

- multiple wireless nodes through which the Internet can be accessed;
- multiple access points with which the wireless nodes can communicate;
- a server configured to receive wireless communication from the multiple access points, the server configured to enable authentication of various users; and
- at least one global authentication database that contains user information that can be used to authenticate the users ***without requiring the users to be affiliated with a particular Internet Service Provider (ISP)***.

Applicant has amended this claim to clarify that user authentication ***does not require*** the users to be affiliated with a particular ISP. In making out the rejection of claim 23, the Office argues that Xu anticipates this claim. However, as noted above, Xu ***does require*** the users to be affiliated with one of the given ISPs before the users can be authenticated. As such, Xu teaches ***directly away*** from Applicant's claimed subject matter. Accordingly, for at least this reason, this claim is allowable.

Claims 24-33 depend from claim 23 and, as such, are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 23, are neither shown nor suggested by Xu either singly or in combination with any of the references of record.

For example, **claim 25** recites that the server is configured to present a ***web page having a link to the one global authentication database***. The Office cites page 13, lines 17-19, of Xu to support its argument that "a user may connect via the World Wide Web." This excerpt is provided below [emphasis added]:

> With the above Figs.1 and 2 and 2A in mind, it will be appreciated that a method of ***connecting a source*** 12 of digital data ***to*** a computer network 24, 22 (e.g., corporate private network, Internet, ***World Wide Web***, etc.) is provided.

However, Applicant can find nothing to indicate, from this excerpt or any other part of Xu's disclosure, that Xu envisions a ***web page having a link to a global authentication database*** as that term is contemplated in Applicant's disclosure. Rather, the World Wide Web appears to be a possible ***destination*** of a user in Xu's system ***after the user is authenticated***. Accordingly, for at least this reason, this claim is allowable.

As another example, **claim 26** recites that the server is ***not privy*** to any of the authentication information that gets passed between the user and the one global authentication database. The Office appears to rely on page 13, lines 23-31, of Xu's disclosure to further its argument that this claim is anticipated by Xu. That particular excerpt was set forth previously and actually discloses a communications chassis which ***is*** privy to authentication information which gets passed between the user and the authentication database. As such, Xu again teaches ***directly away*** from Applicant's claimed subject matter. For at least this reason, this claim is allowable.

In addition, with respect to **claims 30 and 32**, the addition of the Scholnick and Dunn references, respectively, is not seen to add anything of significance given the allowability of the independent claim from which these claims depend.

Claims 34-41

As amended, **claim 34** recites a method of authenticating a user for Internet access, the method comprising [emphasis added]:

- establishing a communication link between a mobile computing device and a server that is configured to provide Internet access;
- contacting a global authentication database that contains user information that can be used to authenticate one or more users;
- authenticating a user using the information that is contained in the global authentication database, ***independent of any user affiliation with any Internet Service Providers (ISPs)***;
- notifying the server that the user has been authenticated; and
- issuing a unique token to the user for use when sending data packets to the server for transmission to the Internet.

This claim has been amended to clarify that the authentication of a user is ***independent of any user affiliation with any ISPs***. In making out the rejection of claim 34, the Office argues that Xu anticipates this claim. However, Xu does not disclose or suggest authentication being configured to take place in a manner that is ***independent of any user affiliation with any Internet Service Providers (ISPs)***.

In support of its argument, the Office cites to page 7, lines 22-24, for the proposition that Xu discloses an authentication component which

allows connection to "any ISP." This excerpt was reproduced as part of a larger excerpt above but is repeated below for the Office's convenience [emphasis added]:

> The architecture also allows the ***Internet Service Provider operating the local communications chassis*** 20 at the central office to provide Internet access for not only the ISP's customers, but also customers of ***other Internet service providers***.

First, Applicant respectfully submits that this excerpt does not state (or even imply) that Xu's system allows connection to "any ISP." Moreover, even if Xu's system did allow connection to any ISP, that would be quite different than Applicant's claimed subject matter. Applicant's authentication is configured to take place in a manner that is ***independent*** of ***any*** user affiliation with ***any*** Internet Service Providers (ISPs). As noted above in the section entitled "Xu's Disclosure", Xu teaches ***directly away*** from Applicant's claimed subject matter by making authentication ***dependent*** upon user ***affiliation with one of the given ISPs*** before the user can be authenticated. Accordingly, for at least this reason, this claim is allowable.

Claims 35-41 depend from claim 34 and, as such, are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 34, are neither shown nor suggested by the references of record either singly or in combination with one another.

For example, **claim 40** recites that the server is ***not privy*** to any authentication information that passes between the user and the

authentication database. As noted above, Xu teaches ***directly away*** from Applicant's claimed subject matter by teaching that its communication chassis ***is*** privy to authentication information that is passed between the client computing device and its locally accessible authentication database. Accordingly, for at least this reason, this claim is allowable.

Claim 42

As amended, **claim 42** recites one or more computer-readable media having computer-readable instructions thereon which, when executed by one or more computers, cause the computers to [emphasis added]:

- establish a wireless communication link between a mobile computing device and a server that is configured to provide Internet access;
- contact a global authentication database that contains user information that can be used to authenticate one or more users;
- authenticate a user using the information that is contained in the global authentication database, ***independent of requiring the user to be affiliated with a particular Internet Service Provider (ISP)***;
- notify the server that the user has been authenticated; and
- issue a unique token to the user for use when sending data packets to the server for transmission to the Internet.

This claim has been amended to clarify that the authentication of a user is ***independent of requiring*** the user to be affiliated with a particular ISP. In making out the rejection of this claim, the Office argues that the subject matter of this claim is anticipated by Xu. However, as noted above, Xu's system is ***dependent on requiring*** the user to be affiliated with one of

the given ISPs before the user can be authenticated. As such, Xu teaches ***directly away*** from Applicant's claimed subject matter. Accordingly, for at least this reason, this claim is allowable.

Claims 43-49

As amended, **claim 43** recites a method of authenticating a user for Internet access, the method comprising [emphasis added]:

- configuring multiple access points to receive wireless communication from multiple wireless nodes through which the Internet can be accessed, the multiple wireless nodes being capable of communicating data packets that are intended for transmission to the Internet;
- configuring a server to wirelessly receive the data packets that are communicated to the multiple access points; and
- configuring a globally accessible database that includes information that can be used to authenticate one or more users that desire to access the Internet, authentication taking place in a manner that ***does not require the one or more users to be affiliated with a particular Internet Service Provider (ISP)***.

Applicant has amended this claim to clarify that authentication ***does not require*** the user to be affiliated with a particular ISP. In making out the rejection of this claim, the Office argues that this claim is anticipated by Xu. However, as noted above, Xu ***does require*** the user to be affiliated with one of the given ISPs before the user can be authenticated. As such, Xu teaches ***directly away*** from Applicant's claimed subject matter. Accordingly, for at least this reason, this claim is allowable.

Claims 44-49 depend from claim 43 and, as such, are allowable as depending from an allowable base claim. These claims are also allowable

for their own recited features which, in combination with those recited in claim 43, are neither shown nor suggested by Xu either singly or in combination with any of the references of record.

For example, **claim 46** recites that the user is linked directly to the globally accessible database and authenticated ***outside of the purview*** of the server. The Office argues that Xu anticipates this claim. Applicant respectfully but strongly disagrees. On page 13, lines 23-31, Xu discloses the following [emphasis added]:

> (1) receiving the digital data at a network access server or communications chassis 20 and ***extracting***, from the digital data, ***network access authentication data*** comprising at least one of the following: (a) a telephone number called by the source 12 of digital data, or (b) a telephone number associated with source of digital data;
>
> (2) ***transmitting the authentication data*** over a local area or wide area computer network connected to the communications device 20 to a network authentication server 32A or 32B for the computer network 24 or 22, the network authentication server linked via the local area or wide area computer network 26 to the communications chassis 20;

Therefore, Xu discloses authenticating a user ***within the purview*** of the server. As such, Applicant respectfully submits that Xu again teaches ***directly away*** from Applicant's claimed subject matter. For at least this reason, this claim is allowable.

Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the

Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 2/17/04

By: _____

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256